UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,

Plaintiff,

v. Case No. 19-CR-02

ALEXANDER BEBRIS,

Defendant.

STIPULATION AS TO TESTIMONY FROM MICROSOFT

The United States of America, by and through its attorneys, Matthew D. Krueger, United States Attorney, and Benjamin W. Proctor and Daniel R. Humble, Assistant United States Attorneys, along with Alexander Bebris, by and through his attorney Jason Luczak, hereby stipulate and agree that if called to testify at the evidentiary hearing set for December 3, 2019, in this matter, Jeff Lilleskare, group manager for security and online safety at Microsoft who has knowledge and experience with the development and use of PhotoDNA, would testify to the following.[1]

1. Microsoft has long viewed a safe online environment as a key selling point for its products and services. In 2002, Bill Gates, co-founder and then-chairman of Microsoft, called on employees to rethink their product development approach and strive to deliver products that are "as available, reliable and secure as standard services such as electricity, water services and telephony." With that directive, Microsoft launched Trustworthy Computing, a long-term, collaborative effort to create and deliver secure, private, and reliable computing experiences for everyone based on sound business practices.

2. Microsoft's work to keep individuals and families safer and more secure online has been part of that effort. Microsoft sees its responsibility in online safety as including technology tools for parents and caregivers, as well as providing public awareness-raising and educational materials to help inform the global public about online risks and how to mitigate them. For instance, Microsoft products such as Windows, Xbox 360, and Windows Phone are equipped with a number of family

[1] The stipulation of the parties does not necessarily mean that the parties agree that the statements herein are indisputable, but only that these statements would be Mr. Lilleskare's testimony.

safety technology tools, such as restrictions on access to explicit content and download-blocking. These features are not legally required, but Microsoft has determined that many customers value such tools. ln addition, the resources at Microsoft's Safety & Security Center and its Digital Skills Program provide customers and the general public with information about protecting children from online bullying, ensuring that young people safely use social media, safeguarding online reputations and other issues related to personal and family online safety. Similarly, to protect the integrity of its services, Microsoft requires users to agree to a Code of Conduct that sets on line community standards, and Microsoft expressly reserves the right to remove content from its services, ban participants, and terminate services. Lastly, Microsoft has made significant investments in protecting its customers and cloud environment through its Digital Crimes Unit ("DCU"). The purpose of the DCU is to fight cybercrime through the innovative application of technology, forensics, law, and partnerships. While some DCU investigations result in evidence that law enforcement can use in criminal investigations, Microsoft did not create the DCU to assist law enforcement, but rather as part of its business-driven strategy to protect its customers and services.

3. PhotoDNA is another element of Microsoft's voluntary business strategy to protect its customers, systems, and reputation by creating a safer online environment. PhotoDNA is an image-matching technology developed by Microsoft in collaboration with Dartmouth College that helps Microsoft find and remove images of child sexual abuse from Microsoft's online services.

4. Microsoft developed and implemented PhotoDNA as a result of its independent judgment that blocking illegal images of child sexual abuse from its services is in Microsoft's business interests. In Microsoft's experience, the direct and indirect costs resulting from the presence of such images can be significant. For example, the presence of such images can increase the volume of consumer complaints received by Microsoft and, potentially, cause substantial harm to Microsoft's image and reputation in the marketplace. Microsoft believes that its customers are entitled to safer and more secure online experiences that are free of images depicting child sexual abuse. For these reasons, Microsoft devotes resources and develops and deploys technology, including PhotoDNA, to prevent the transmission and storage of images of child sexual abuse on Microsoft's services.

5. No government agency or law enforcement officer directed or requested that Microsoft create or use PhotoDNA.

6. PhotoDNA uses a mathematical algorithm to create a unique signature—similar to a fingerprint—for each digital image. It does this by adjusting the image to a standard size for processing; converting the image into black and white and breaking the image into sections; calculating a unique number to represent each section, and then placing all those numbers together to create a

single code that uniquely represents that image. That code is a unique signature for the digital image, which can be compared with the signatures of other images to find copies of the original image.

7. The technique described in the above paragraph is known as "hashing." PhotoDNA's robust hashing differs from other hashing technologies because the PhotoDNA signature is based on the essence of the image and not the specific electronic file containing the image. Therefore, if an image has been resized, recolored, saved in a different file format or otherwise similarly altered, PhotoDNA can still reliably identify copies of the image when other hashing technologies (that require every file characteristic to be precisely the same) could not.

8. Microsoft uses PhotoDNA on several of its services to scan certain user-generated content against a database of hashes of known images of child sexual abuse.

9. If the hash of scanned content matches the hash of a known image of child sexual abuse (also known as a "hit"), Microsoft takes several steps to prevent the continued access to and/or transmission of the images, to protect its customers, and to report the images as required by law. First, it suspends the account, such that the customer no longer has access to or use of the account or any other Microsoft online services associated with the account. Second, as required by federal law, Microsoft files a CyberTipline report with the National Center for Missing and Exploited Children ("NCMEC"). The report may contain basic information about the PhotoDNA match, including the file names, Internet Protocol (IP) address(es) associated with the account, and the name and email address that the customer provided when registering the account.

10. Microsoft makes the PhotoDNA program available without charge to qualified companies, since the use of this service contributes to Microsoft's business goal of creating a safer online experience. To this end, Microsoft has licensed PhotoDNA to Facebook. With this license, Facebook has the same technical capability to scan content against databases of known child pornography files as described above.

11. Neither NCMEC nor any government agency ever asked Microsoft to search any files associated with this case.

12. No government agency or law enforcement officer directed or requested that Microsoft create or use PhotoDNA. Nor did Microsoft create these technologies at the request of the NCMEC.

13. With regard to PhotoDNA and NCMEC, as noted, PhotoDNA was the product of a collaboration between Microsoft and a computer science professor at

Dartmouth College. NCMEC was also working to combat child sexual exploitation, and so Microsoft consulted NCMEC as part of the process—along with other companies, non-profits, and academics. Then, after the development of PhotoDNA, Microsoft licensed the technology to NCMEC at no cost, which enabled that organization to generate the original set of PhotoDNA hash values. Microsoft also licensed PhotoDNA to other companies for testing and evaluation. Thus, while NCMEC (along with other private companies, non-profits, and academics) was a resource for Microsoft, NCMEC was not responsible for the actual development or implementation of PhotoDNA.